```
  ***************************************************************************
  ***************************************************************************
  ************************ NEWBIES HANDBOOK ******************************
  ************** HOW TO BEGIN IN THE WORLD OF H/P ************************
  ************************ BY : Plowsk Phreak ************************************
  ***************************************************************************
  ***************************************************************************
```

Disclaimer-
I am not responsible for any of the information in this document, if it is used for any other purpose than educational reading. Some of the information on this page can be used illegally if the reader does not act responsible. The reader is responsible for his own actions.
You can copy anything from this file to any other file as long as you quote, dont change it up, and give me the proper credit...like:
NEWBIES HANDBOOK
HOW TO BEGIN IN THE WORLD OF H/P
BY : Plowsk Phreak
Into:

When I got into hacking, i realized that there wasnt many text philes for newbies. so, i decided to write one. i dont really care about misspelled werds or puncuation so, please ignore the mistakes. In this document i will refer you to other documents a lot. (because why should i waste my time rewriting something that has already been writen?) If at anytime while reading this document you ask yourself "So...How do I hack?", then go away now and save yourself the frustration because you'll never learn. To hack you must understand everything about a system, and then you can get ideas and try them out.

I tried to keep this phile as short as possible, when you read this you should just get an idea about how to hack and why we hack. If you read this document and the philes that i have listed, you should have a good idea on what to do, how to do it, and why. Remember every 'project' is different. You have to use your brain and adjust to each different one.
Tools:

There are a few things you need to have to be a hacker/phreaker.
'puter - computer (duh)
terminal software - a program like, hyper terminal or ordinary terminal that allows you to dial out to another system.
blue box - (exerpted from 2600faq)Blue boxes use a 2600hz tone to size control of telephone switches that use in-band signalling. The caller may then access special switch functions, with the usual purpose of making free long distance phone calls, using the tones provided by the Blue Box.

scanner - a scanner is a program that dials out every number in your area and listens for tones that are comming from other modems. (helps you locate your local targets) a good scanner is Toneloc. Find it!
Fone (phone) line - I hope you know whut this is...
It also helps to know a computer language ex: C, C++ ect.

Info resources:
I dont know many good boards anymore because almost all of their sysops (system operators) have been busted. But I suggest you get a server that uses netscape and get unlimited access to the www(World wide web). And visit these good homepages by entering their name in the webcrawler search engine (http://webcrawler.com)

Silicon Toads Hacking Resources
Flamestrike Enterprises
The Plowsk Page (mine, you can reach me from there)
Matervas Hideout
Burns Lair

Cold fire
  From these pages you will find a wealth of information on h/p
(hacking/phreaking)

getting started:
 the first thing you must do is get on your computer, open your terminal software and connect to a board. (bulletin board, bbs). This is a must! (its also a VERY basic thing). (You can usually find a bbs number on a homepage or enter bbs in a search engine.) Now that you can do that, start reading. Read as many text philes as possible.
Required reading:
Hackers Manifesto (at bottom)
Hackers Code of ethics
Any old issues of Phrack
any old issues of 2600
2600faq
any text documents on systems (unix, iris, dec)
DOD (department of defense) standards
Any philes on boxes (blue(one at bottom), red, beige)

For beginners, which most of you probably are, I suggest you find some of the following systems that exist in your area and work on them first. (they are the easiest and least risky)
This next segment is excerpted from:
A Novice's Guide to Hacking- 1989 edition
by
The Mentor
Legion of Doom/Legion of Hackers

IRIS- IRIS stands for Interactive Real Time Information System. It originally ran on PDP-11's, but now runs on many other minis. You can spot an IRIS by the 'Welcome to "IRIS" R9.1.4 Timesharing' banner, and the ACCOUNT ID? prompt. IRIS allows unlimited tries at hacking in, and keeps no logs of bad attempts. I don't know any default passwords, so just try the common ones from the password database below.
Common Accounts:
MANAGER
BOSS
SOFTWARE
DEMO
PDP8
PDP11
ACCOUNTING

DEC-10- An earlier line of DEC computer equipment, running the TOPS-10 operating system. These machines are recognized by their '.' prompt. The DEC-10/20 series are remarkably hacker-friendly, allowing you to enter several important commands without ever logging into the system. Accounts are in the format [xxx,yyy] where xxx and yyy are integers. You can get a listing of the accounts and the process names of everyone on the system before logging in with the command .systat (for SYstem STATus). If you seen an account that reads [234,1001] BOB JONES, it might be wise to try BOB or JONES or both for a password on this account. To login, you type .login xxx,yyy and then type the password when prompted for it. The system will allow you unlimited tries at an account, and does not keep records of bad login attempts. It will also inform you if the UIC you're trying (UIC = User Identification Code, 1,2 for example) is bad.
Common Accounts/Defaults:
1,2: SYSLIB or OPERATOR or MANAGER
2,7: MAINTAIN
5,30: GAMES

UNIX- There are dozens of different machines out there that run UNIX. While some might argue it isn't the best operating system in the world, it is certainly the most widely used. A UNIX system will usually have a prompt like 'login:' in lower case. UNIX also will give you unlimited shots at logging in (in most cases), and there is usually no log kept of bad attempts.

Common Accounts/Defaults: (note that some systems are case sensitive, so use lower case as a general rule. Also, many times the accounts will be unpassworded, you'll just drop right in!)

root:	root
admin:	admin
sysadmin:	sysadmin or admin
unix:	unix
uucp:	uucp
rje:	rje
guest:	guest
demo:	demo
daemon:	daemon
sysbin:	sysbin

Code of ethics:

Once you get in a system, do not manipulate anything but the log file (erase the record of your bad logins) and anywhere you might have left your handle. (name, a.k.a.) You dont want to leave your handle anywhere because they WILL be able to track you down by your handle alone.

Its ok to be paranoid!

Dont think for one minute that you are undetectable, if you make any mistakes, you could get caught. Here is a list of things you could do to help yourself from getting in trouble.

* Encrypt your entire hard drive
* hide your files in a very safe spot.
* dont tell anyone that you dont know very well about your hacking. Good hackers never reveal specific details to anyone about their current project. They give only very vague hints of what they are doing.
* dont openly give out your real name or address
* dont join any major hacking groups, be an individual.
* Dont hack government computers, ESPECIALLY YOUR OWN GOVERNMENTS! Foreign computers can sometimes be phun, but dont say i didnt warn you!
* Make sure that you dont leave any evidence that you have been in a system and any evidence of who it was.
* Use your brain.

If you follow most of these guidelines, you should be safe. The last thing you want is to end up in a one room apartment located in the third floor of the state prision with your cellmate Bruno, the ax murderer, whose doing life.

Getting in:

The hardest thing about hacking is getting the numbers for a system. You can do this by using a scanning program. Then, once you connect to a system you must first recognise what kind of system you have connected to. (by the way, for you real brainiacs, you have to use your terminal software to call another system.) You can usually do this by looking at the prompt you get, if you get one. (check the Unresponsive section) Sometimes a system will tell you as soon as you connect by saying some thing like "hello, welcome to Anycompany using anysystem v 1.0" When you determine what system you have connected to, this is when you start trying your logins. You can try typing in demo and as your userid and see if you can find any users names to try. If you enter a name and you are allowed in without a password you usually, but not always, have entered a name that you cant do a whole lot with but, it can still be phun and you can probably find clues on how to get in on another name.

While your in:

There are usually many interesting files you can read in all of these systems. You can read files about the system. You might want to try a help

command. They will usually tell you a lot. Sometimes, if your lucky, you can manage to download the manual of the system!
There is nothing like the thrill of your first hack, even if it wasnt a very good one, it was probably still phun. You could read every text phile in the world and you still probably wouldnt learn as much as you do during your first hack. Have Phun!
This next segment is also excerpted from:
A Novice's Guide to Hacking- 1989 edition
by
The Mentor
Legion of Doom/Legion of Hackers

Unresponsive Systems
~~~~~~~~~~~~~~~~~~~~

Occasionally you will connect to a system that will do nothing but sit there. This is a frustrating feeling, but a methodical approach to the system will yield a response if you take your time. The following list will usually make *something* happen.

1) Change your parity, data length, and stop bits. A system that won't respond at 8N1 may react at 7E1 or 8E2 or 7S2. If you don't have a term program that will let you set parity to EVEN, ODD, SPACE, MARK, and NONE, with data length of 7 or 8, and 1 or 2 stop bits, go out and buy one. While having a good term program isn't absolutely necessary, it sure is helpful.
2) Change baud rates. Again, if your term program will let you choose odd baud rates such as 600 or 1100, you will occasionally be able to penetrate some very interesting systems, as most systems that depend on a strange baud rate seem to think that this is all the security they need...
3) Send a series of <cr>'s.
4) Send a hard break followed by a <cr>.
5) Type a series of .'s (periods). The Canadian network Datapac responds to this.
6) If you're getting garbage, hit an 'i'. Tymnet responds to this, as does a MultiLink II.
7) Begin sending control characters, starting with ^A --> ^Z.
8) Change terminal emulations. What your vt100 emulation thinks is garbage may all of a sudden become crystal clear using ADM-5 emulation. This also relates to how good your term program is.
9) Type LOGIN, HELLO, LOG, ATTACH, CONNECT, START, RUN, BEGIN, LOGON, GO, JOIN, HELP, and anything else you can think of.
10) If it's a dialin, call the numbers around it and see if a company answers. If they do, try some social engineering.

I tried to keep this phile as short as possible to save downloading time and just telling you the very basics like what you need to do and what you need to read. I hope this was helpful.

Plowsk Phreak
Here are two philes i copied for your reading pleasure:
bluebox.txt
and
The Hackers Manifesto
bluebox.txt -
The Secrets of the Little Blue Box Originally found in Esquire Magazine
THE BLUE BOX IS INTRODUCED: IT'S QUALITIES ARE REMARKED
I am in the expensively furnished living room of Al Gilbertson, the creator of the blue box. Gilbertson is holding one of his shiny black-and-silver blue boxes comfortably in the palm of his hand, pointing out the thirteen little red push buttons sticking up from the console. He is dancing his fingers over the buttons, tapping out discordant beeping electronic jingles. He is trying to explain to me how his little blue box does nothing less than place the entire telephone system of the world, satellites, cables and all, at the service of the blue-box operator, free of charge.
"That's what it does. Essentially it gives you the power of a super operator. You sieze a tandem with this top button," he presses the top
~~~~~~~~~~~~~~~~~~~~

button with his index finger and the blue box emits a high-pitched cheep, "and like that," the box cheeps again "you control the phone company's long distance switching systems from your cute little Princess phone or any old pay phone. And you've got anonymity. An operator has to operate from a definite location. The phone company knows where she is and what she's doing. But with your blue box, once you hop onto a trunk, say from a Holiday Inn 800 number, they don't know where you are, or where you're coming from, they don't know how you slipped into their lines and popped up in that 800 number. They don't even know anything illegal is going on. And you can obscure your origins through as many levels as you like. You can call next door by way of White Plains, then over to Liverpool by cable and then back here by satellite. You can call yourself from one pay phone all the way around the world to a pay phone next to you. And you get your dime back too.
"And they can't trace the calls? They can't charge you?"
"Not if you do it the right way. But you'll find that the free-call thing isn't really as exciting at first as the feeling of power you get from having one of these babies in your hand. I've watched people when they first get hold of one of these things and start using it, and discover they can make connections, set up crisscross and zigzag switching patterns back and forth across the world. They hardly talk to the people they finally reach. They say hello and start thinking of what kind of call to make next. They go a little crazy." He looks down at the neat little package in his palm. His fingers are still dancing, tapping out beeper patterns.
"I think it's something to do with how small my models are. There are lots of blue boxes around, but mine are the smallest and most sophisticated electronically. I wish I could show you the prototype we made for our big syndicate order."
He sighs. "We had this order for a thousand blue boxes from a syndicate front man in Las Vegas. They use them to place bets coast to coast, keep lines open for hours, all of which can get expensive if you have to pay. The deal was a thousand blue boxes for $300 apiece. Before then we retailed them for $1500 apiece, but $300,000 in one lump was hard to turn down. We had a manufacturing deal worked out in the Philippines. Everything was ready to go. Anyway, the model I had ready for limited mass production was small enough to fit inside a flip-top Marlboro box. It had flush-touch panels for a keyboard, rather than these unsightly buttons sticking out. Looked just like a tiny portable radio. In fact I had designed it with a tiny transistor receiver to get one AM channel, so in case the law became suspicious the owner could switch on the radio part, start snapping his fingers and no one could tell anything illegal was going on. I thought of everything for this model--I had it lined with a band of thermite which could be ignited by radio signal from a tiny button transmitter on your belt, so it could be burned to ashes instantly in case of a bust. It was beautiful. A beautiful little machine. You should have seen the face on these syndicate guys when they came back after trying it out. They'd hold it in their palm like they never wanted to let it go, and they'd say, 'I can't believe it.' You probably won't believe it until you try it."
THE BLUE BOX IS TESTED: CERTAIN CONNECTIONS ARE MADE
About eleven o'clock two nights later Fraser Lucey has a blue box in the palm of his left hand and a phone in the palm of his right. His is standing inside a phone booth next to an isolated shut-down motel. I am standing outside the phone booth.
Fraser likes to show off his blue box for people. Until a few weeks ago when Pacific Telephone made a few arrests in his city, Fraser Lucey liked to bring his blue box to parties. It never failed: a few cheeps from his device and Fraser became the center of attention at the very hippest of gatherings, playing phone tricks and doing request numbers for hours. He began to take orders for his manufacturer in Mexico. He became a dealer.
Fraser is cautious now about where he shows off his blue box. But he never gets tired of playing with it. "It's like the first time every time," he tells me.
Fraser puts a dime in the slot. He listens for a tone and holds the receiver up to my ear. I hear the tone.
Fraser begins describing, with a certain practiced air, what he does while

he does it.
"I'm dialing an 800 number now. Any 800 number will do. It's toll free. Tonight I think I'll use the Ryder Rent A Van number. Listen it's ringing. Here, you hear it? Now watch."
He places the blue box over the mouthpiece of the phone so that the one silver and twelve black push buttons are facing up toward me. He presses the silver button - the one at the top - and I hear that high-pitched beep.
"That's 2600 cycles per second to be exact," says Lucey. "Now, quick, listen."
He shoves the ear piece at me. The ringing has vanished. The line gives a slight hiccough, there is a sharp buzz, and then nothing but soft white noise.
"We're home free now," Lucey tells me, taking back the phone and applying the blue box to its mouthpiece once again. "We're up on a tandem, into a long-lines trunk. Once you're up on a tandem, you can send yourself anywhere you want to go." He decides to check you London first. He chooses a certain pay phone located in Waterloo station. This particular pay phone is popular with the phone-phreaks because there are usually people walking by at all hours who will pick it up and talk for a while.
He presses the lower left-hand corner button which is marked "KP" on the face of the box.
"That's Key Pulse. It tells the tandem we're ready to give it instructions. First I'll punch out KP 182 START, which will slide us into the overseas sender in White Plains." I hear neat clunk-cheep. "I think we'll head over to England by satellite. Cable is actually faster and the connection is somewhat better, but I like going by satellite. So I just punch out KP Zero 44. The Zero issupposed to guarantee a satellite connection and 44 is the country code for England. Okay...we're there. In Liverpool actually. Now all I have to do is punch out the London area code which is 1, and dial up the pay phone. Here, listen, I've got a ring now."
I hear the soft quick purr-purr of a London ring. Then someone picks up the phone. "Hello," says the London voice.
"Hello, Who's this?" Fraser asks.
"Hello. There's actually nobody here. I just picked this up while I was passing by. This is a public phone. There's no one here to answer actually."
"Hello. Don't hang up. I'm calling from the United States."
"Oh. What is the purpose of the call? This is a public phone you know."
"Oh. You know. To check out, uh, to find out what's going on in London. How is it there?"
"It's five o'clock in the morning. It's raining now."
"Oh. Who are you?"
The London passerby turns out to be an R.A.F. enlistee on his way back to the base in Lincolnshire, with a terrible hangover after a thirty-six hour pass.
He and Fraser talk about the rain. They agree that it's nicer when it's not raining. They say good-bye and Fraser hangs up. His dime returns with a nice clink.
"Isn't that far out," he says grinning at me. "London. Like that."
Fraser squeezes the little blue box affectionately in his palm. "I told ya this thing is for real. Listen, if you don't mind I'm gonna try this girl I know in Paris. I usually give her a call around this time. It freaks her out. This time I'll use the Penske 800 number and we'll go by overseas cable 133; 33 is the country code for France, the 1 sends you by cable. Okay, here we go. Oh damn. Busy. Who could she be talking to at this time?"
A state police car cruises slowly by the motel. The car does not stop, but Fraser gets nervous. We hop back into his car and drive ten miles in the opposite direction until we reach a Texaco station locked up for the night. We pull up to a phone booth by the tire pump. Fraser dashes inside and tries the Paris number. It is busy again.
"I don't understand who she could be talking to. The circuits may be busy. It's too bad I haven't learned how to tap into lines overseas with this thing yet."
Fraser begins to phreak around, as the phone phreaks say. He dials a leading nationwide charge card's 800 number and punches out the tones that bring him

the Time recording in Sydney, Australia. He beeps up the Weather recording in Rome, in Italian of course. He calls a friend in Chicago and talks about a certain over the counter stock they are into heavily. He finds the Paris number busy again. He calls up a dealer of another sort and talks in code. He calls up Joe Engressia, the original blind phone phreak genius, and pays his respects. There are other calls. Finally Fraser gets through to his young lady in Paris. They both agree the circuits must have been busy, and criticize the Paris telephone system. At two-thirty in the morning Fraser hangs up, pockets his dime, and drives off, steering with one hand, holding what he calls his "lovely little blue box" in the other.

YOU CAN CALL LONG DISTANCE FOR LESS THAN YOU THINK

"You see, a few years ago the phone company made one big mistake," Gilbertson explains two days later in his apartment. "They were careless enough to let some technical journal publish the actual frequencies used to create all their multi-frequency tones. Just a theoretical article some Bell Telephone Laboratories engineer was doing about switching theory, and he listed the tones in passing. At MIT I had been fooling around with phones for several years before I came across a copy of the journal in the engineering library. I ran back to the lab and it took maybe twelve hours from the time I saw that article to put together the first working blue box. It was bigger and clumsier than this little baby, but it worked."

It's all there on public record in that technical journal written mainly by Bell Lab people for other telephone engineers. Or at least it was public.

"Just try and get a copy of that issue at some engineering school library now. Bell has had them all red-tagged and withdrawn from circulation," Gilbertson tells me.

"But it's too late now. It's all public now. And once they became public the technology needed to create your own beeper device is within the range of any twelve-year-old kid, any twelve-year-old blind kid as a matter of fact. And he can do it in less than the twelve hours it took us. Blind kids do it all the time. They can't build anything as precise and compact as my beeper box, but theirs can do anything mine can do."

"How?"

"Okay. About twenty years ago AT&T made a multi-million dollar decision to operate its entire long-distance switching system on twelve electronically generated combinations of six master tones. Those are the tones you sometimes hear in the background after you've dialed a long distance number. They decided to use some very simple tones. The tone for each number is just two fixed single-frequency tones played simultaneously to create a certain beat frequency. Like 1300 cycles per second and 900 cycles per second played together give you the tone for digit 5. Now, what some of these phone phreaks have done is get themselves access to an electric organ. Any cheap family home entertainment organ. Since the frequencies are public knowledge now, one blind phone phreak has even had them recorded in one of those talking books for the blind, they just have to find the musical notes on the organ which correspond to the phone tones. Then they tape them. For instance, to get Ma Bell's tone for the number, you press down organ keys F3 and A3 (900 and 700 cycles per second) at the same time. To produce the tone for 2 it's F3 and C6 (1100 and 700 c.p.s). The phone phreaks circulate the whole list of notes so there's no trial and error anymore."

He shows me a list of the rest of the phone numbers and the two electric organ keys that produce them.

"Actually, you have to record these notes at 3 3/4 inches per second tape speed and double it to 7 1/2 inches per second when you play them back, to get the proper tones," he adds.

"So once you have all the tones recorded, how do you plug them into the phone system?"

"Well, they take their organ and their cassette recorder, and start banging out entire phone numbers in tones on the organ, including country codes, routing instructions, 'KP' and 'Start' tones. Or, if they don't have an organ, someone in the phone-phreak network sends them a cassette with all the tones recorded with a voice saying 'Number one,' then you have the tone, 'Number two,' then the tone and so on. So with two cassette recorders they can put together a series of phone numbers by switching back and forth from

number to number. Any idiot in the country with a cheap cassette recorder can make all the free calls he wants."
"You mean you just hold the cassette recorder up to the mouthpiece and switch in a series of beeps you've recorded? The phone thinks that anything that makes these tones must be its own equipment?"
"Right. As long as you get the frequency within thirty cycles per second of the phone company's tones, the phone equipment thinks it hears its own voice talking to it. The original grandaddy phone phreak was this blind kid with perfect pitch, Joe Engressia, who used to whistle into the phone. An operator could tell the difference between his whistle and the phone company's electronic tone generator, but the phone company's switching circuit can't tell them apart.
The bigger the phone company gets and the further away from human operators it gets, the more vulnerable it becomes to all sorts of phone Phreaking."
A GUIDE FOR THE PERPLEXED
"But wait a minute," I stop Gilbertson. "If everything you do sounds like phone-company equipment, why doesn't the phone company charge you for the call the way it charges its own equipment?"
"Okay. That's where the 2600-cycle tone comes in. I better start from the beginning."
The beginning he describes for me is a vision of the phone system of the continent as thousands of webs, of long-line trunks radiating from each of the hundreds of toll switching offices to the other toll switching offices. Each toll switching office is a hive compacted of thousands of long-distance tandems constantly whistling and beeping to tandems in far-off toll switching offices.
The tandem is the key to the whole system. Each tandem is a line with some relays with the capability of signaling any other tandem in any other toll switching office on the continent, either directly one-to-one or by programming a roundabout route several other tandems if all the direct routes are busy. For instance, if you want to call from New York to Los Angeles and traffic is heavy on all direct trunks between the two cities, your tandem in New York is programmed to try the next best route, which may send you down to a tandem in New Orleans, then up to San Francisco, or down to a New Orleans tandem, back to an Atlanta tandem, over to an Albuquerque tandem and finally up to Los Angeles.
When a tandem is not being used, when it's sitting there waiting for someone to make a long-distance call, it whistles. One side of the tandem, the side "facing" our home phone, whistles at 2600 cycles per second toward all the home phones serviced by the exchange, telling them it is at their service, should they be interested in making a long-distance call. The other side of the tandem is whistling 2600 c.p.s. into one or more long distance trunk lines, telling the rest of the phone system that it is neither sending nor receiving a call through the trunk at the moment, that it has no use for that trunk at the moment.
When you dial a long-distance number the first thing that happens is that you are hooked into a tandem. A register comes up to the side of the tandem facing away from you and presents that side with the number you dialed. This sending side of the tandem stops whistling 2600 into its trunk line. When a tandem stops the 2600 tone it has been sending through a trunk, the trunk is said to be "seized," and is now ready to carry the number you have dialed, converted into multi-frequency beep tones, to a tandem in the area code and central office you want.
Now when a blue-box operator wants to make a call from New Orleans to New York he starts by dialing the 800 number of a company which might happen to have its headquarters in Los Angeles. The sending side of this New Orleans tandem stops sending 2600 out over the trunk to the central office in Los Angeles, thereby seizing the trunk. Your New Orleans tandem begins sending beep tones to a tandem it has discovered idly whistling 2600 cycles in Los Angeles. The receiving end of that L.A. tandem is seized, stops whistling 2600, listens to the beep tones which tell it which L.A. phone to ring, and starts ringing the 800 number. Meanwhile, a mark made in the New Orleans office accounting tape indicates that a call from your New Orleans phone to the 800 number in L.A. has been initiated and gives the call a code number.

Everything is routine so far.
But then the phone phreak presses his blue box to the mouthpiece and pushes the 2600-cycle button, sending 2600 out from the New Orleans tandem notices the 2600 cycles are coming over the line again and assumes that New Orleans has hung up because the trunk is whistling as if idle. But,
Thus the blue-box operator in New Orleans now is in touch with a tandem in L.A. which is waiting like and obedient genie to be told what to do next. The blue-box owner then beeps out the ten digits of the New York number which tells the L.A. tandem to relay a call to New York City. Which it promptly does. As soon as your party picks up the phone in New York, the side of the New Orleans tandem facing you stops sending 2600 to you and starts carrying his voice to you by way of the L.A. tandem. A notation is made on the accounting tape that the connection has been made on the 800 call which had been initiated and noted earlier. When you stop talking to New York a notation is made that the 800 call has ended.
At three the next morning, when phone company's accounting computer starts reading back over the master accounting tape for the past day, it records that a call of a certain length of time was made from your New Orleans home to an L.A. 800 number and, of course the accounting computer has been trained to ignore these toll free 800 calls when compiling your monthly bill.
"All they can prove is that you made an 800 call," Gilbertson the inventor concludes. "Of course, if you're foolish enough to talk for two hours on an 800 call, and they've installed one of their special anti-fraud computer programs to watch out for such things, they may spot you and ask you why you took two hours talking to Army Recruiting's 800 number when you're 4-F. But if you do it from a pay phone, they may discover something peculiar the next day, if they've got a blue-box hunting program in their computer, but you'll be a long time gone from the pay phone by then. Using a pay phone is almost guaranteed safe."
"What about the recent series of blue-box arrests all across the country, New York, Cleveland, and so on?" I asked. "How were they caught so easily?"
"From what I can tell, they made one big mistake. They were seizing trunks using an area code plus 555-1212 instead of an 800 number. When you send multi-frequency beep tones off 555 you get a charge for it on your tape and the accounting computer knows there's something wrong when it tries to bill you for a two-hour call to Akron, Ohio, information, and it drops a trouble card which goes right into the hands of the security agent if they're looking for blue-box users.
"Whoever sold those guys their blue boxes didn't tell them how to use them properly, which is fairly irresponsible. And they were fairly stupid to use them at home all the time. But what those arrests really mean is that an awful lot of blue boxes are flooding into the country and that people are finding them so easy to make that they know how to make them before they know how to use them. Ma Bell is in trouble."
"And if a blue-box operator or a cassette-recorder phone phreak sticks to pay phones and 800 numbers, the phone company can't stop them?"
"Not unless they change their entire nationwide long-lines technology, which will take them a few billion dollars and twenty years. Right now they can't do a thing. They're screwed."
CAPTAIN CRUNCH DEMONSTRATES HIS FAMOUS UNIT
There is an underground telephone network in this country. Gilbertson discovered it the very day news of his activities hit the papers. That evening his phone began ringing. Phone phreaks from Seattle, from Florida, from New York, from San Jose, and from Los Angeles began calling him and telling him about the phone-phreak network. He'd get a call from a phone phreak who'd say nothing but, "Hang up and call this number."
When he dialed the number he'd find himself tied into a conference of a dozen phone phreaks arranged through a quirky switching station in British Columbia. They identified themselves as phone phreaks, they demonstrated their homemade blue boxes which they called "MFers"(for multi-frequency, among other things) for him, they talked shop about phone phreak devices. They let him in on their secrets on the theory that if the phone company was after him he must be trustworthy. And, Gilbertson recalls, they stunned him

with their technical sophistication.
I ask him how to get in touch with the phone-phreak network. He digs around through a file of old schematics and comes up with about a dozen numbers in three widely separated area codes.
"Those are the centers," he tells me. Alongside some of the numbers he writes in first names or nicknames: names like Captain Crunch, Dr. No, Frank Carlson, (also a code word for free call), Marty Freeman (code word for MF

device), Peter the Perpendicular Pimple, Alefnull, and The Cheshire Cat. He makes checks alongside the names of those among these top twelve who are blind. There are five checks.
I ask him who this Captain Crunch person is.
"Oh, The Captain. He's probably the most legendary phone phreak. He calls himself Captain Crunch after the notorious Cap'n Crunch 2600 whistle. Several years ago the makers of Cap'n Crunch breakfast cereal offered a toy whistle prize in every box as a treat for the Cap'n Crunch set. Somehow a phone phreak discovered that the toy whistle just happened to produce a perfect 2600-cycle tone. When the man who calls himself Captain Crunch was transferred overseas to England with his Air Force unit, he would receive scores of calls from his friends and "mute" them, that is, make them free of charge to them, by blowing his Cap'n Crunch whistle into his end."
"Captain Crunch is one of the older phone phreaks," Gilbertson tells me. "He's an engineer who once got in a little trouble for fooling around with the phone, but he can't stop. Well, this guy drives across country in a Volkswagen van with an entire switchboard and a computerized super-sophisticated MFer in the back. He'll pull up to a phone booth on a lonely highway somewhere, snake a cable out of his bus, hook it onto the phone and sit for hours, days sometimes, sending calls zipping back and forth across the country, all over the world."
Back at my house, I dialed the number he gave me for "Captain Crunch" and asked for Gary Thomas, his real name, or at least the name he uses when he's not dashing into a phone booth beeping out MF tones faster than a speeding bullet, and zipping phantomlike through the phone company's long-distance lines.
When Gary answered the phone and I told him I was preparing a text file about phone phreaks, he became very indignant.
"I don't do that. I don't do that anymore at all. And if I do it, I do it for one reason and one reason only. I'm learning about a system. The phone company is a system. A computer is a system. Do you understand? If I do what I do, it is only to explore a System. Computers. Systems. That's my bag. The phone company is nothing but a computer."
A tone of tightly restrained excitement enters the Captain's voice when he starts talking about Systems. He begins to pronounce each syllable with the hushed deliberation of an obscene caller.
"Ma Bell is a system I want to explore. It's a beautiful system, you know, but Ma Bell screwed up. It's terrible because Ma Bell is such a beautiful system but she screwed up. I learned how she screwed up from a couple of blind kids who wanted me to build a device. A certain device. They said it could make free calls. But when these blind kids told me I could make calls into a computer, my eyes lit up. I wanted to learn about computers. I wanted to learn about Ma Bell's computers. So I built the little device. Only I built it wrong and Ma Bell found out. Ma Bell can detect things like that. Ma Bell knows. So I'm strictly out of it now. I don't do it. Except for learning purposes." He pauses. "So you want to write a text file. Are you paying for this call? Hang up and call this number."
He gives me a number in an area code a thousand miles north of his own. I dial the number.
"Hello again. This is Captain Crunch. You are speaking to me on a toll-free loop in Portland Oregon. Do you know what a toll-free loop is? I'll tell you."
He explains to me that almost every exchange in the country has open test numbers which allow other exchanges to test their connections with it. Most of thest numbers occur in consecutive pairs, such as 302 956-0041 and 956-0042. Well certain phone phreaks discovered that if two people from

anywhere in the country dial those two consecutive numbers they can talk together just as if one had called the other's number, with no charge to either of them, of course.
"Your voice is looping around in a 4A switching machine up there in Canada, zipping back down to me," the Captain tells me. "My voice is looping around up there and back down to you. And it can't ever cost anyone money. The phone phreaks and I have compiled a list of many many of these numbers. You would be surprised if you saw the list. I could show it to you. But I won't. I'm out of that now. I'm not out to screw Ma Bell. I know better. If I do anything it's for the pure knowledge of the System. You can learn to do fantastic things. Have you ever heard eight tandems stacked up? Do you know the sound of tandems stacking and unstacking? Give me your phone number. Hang up now and wait a minute.
Slightly less than a minute later the phone rang and the Captain was on the line, his voice sounding far more excited, almost aroused.
"I wanted to show you what it's like to stack up tandems (Whenever the Captain says "stack up" he sounds like he is smacking his lips)."
"How do you like the connection you're on now?" the Captain asks me. "It's a raw tandem. A raw tandem. I'm going to show you what it's like to stack up. Blow off. Land in a faraway place. To stack that tandem up, whip back and forth across the country a few times, then shoot on up to Moscow."
"Listen," Captain Crunch continues. "Listen. I've got a line tie on my switchboard here, and I'm gonna let you hear me stack and unstack tandems. Listen to this. I'm gonna blow your mind."
First I hear a super rapid-fire pulsing of flutelike phone tones, then a pause, then another popping burst of tones, then another, then another. Each burst is followed by a beep-kachink sound.
"We have now stacked up four tandems," said Captain Crunch, sounding somewhat remote. "That's four tandems stacked up. Do you know what that means? That means I'm whipping back and forth, back and forth twice, across the country, before coming to you. I've been known to stack up twenty tandems at a time. Now, just like I said, I'm going to shoot up to Moscow."
There is a new longer series of beeper pulses over the line, a brief silence, then a ring.
"Hello," answers a far-off voice.
"Hello, Is this the American Embassy Moscow?"
"Yes, sir, who is calling?" says the voice.
"Yes, This is test board here in New York. We're calling to check out the circuits, see what kind of lines you've got. Everything okay there in Moscow?"
"Okay?"
"Well, yes, how are things there?"
"Oh. Well everything's okay, I guess."
"Okay. Thank you." They hang up, leaving a confused series of beep-kachink sounds hanging in mid-ether in the wake of the call before disolving away.

Hackers Manifesto -
Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...
Damn kids. They're all alike.
But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?
I am a hacker, enter my world...
Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...
Damn underachiever. They're all alike.
I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."
Damn kid. Probably copied it. They're all alike.
I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me...

Or feels threatened by me...
Or thinks I'm a smart ass...
Or doesn't like teaching and shouldn't be here...
Damn kid. All he does is play games. They're all alike.
And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found.
"This is it... this is where I belong..."
I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...
Damn kid. Tying up the phone line again. They're all alike...
You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.
This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.
Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.
I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

+++The Mentor+++